

## Der Schutz der Menschenrechte im Cyberspace durch die EMRK

Aktuelle Beschwerden beim EGMR im Hinblick auf  
staatliche Überwachung

LAYLA KRISTINA JABER — 7 December, 2016



Der EGMR hat im Laufe seiner Rechtsprechung die „offline“ Gewährleistungen aus dem Recht auf Achtung des Privat- und Familienlebens aus Art. 8 EMRK und dem Recht auf freie Meinungsäußerung aus Art. 10 EMRK auf die neuen Verhaltensweisen im Cyberspace übertragen. Schon seit dem Urteil Klass gg. Deutschland aus dem Jahr 1978 hat er die

Verpflichtung der Mitgliedstaaten zur organisatorischen und verfahrensrechtlichen Sicherung der Privatsphäre und der Einrichtung von geeigneten und effektiven Kontrollinstanzen aus Art. 8 EMRK hergeleitet und hat damit den Weg für den Schutz der Privatsphäre im digitalen Zeitalter geebnet. Ebenso bei der Speicherung von persönlichen Daten im Interesse der nationalen Sicherheit infolge einer heimlichen Überwachung sind die Staaten dazu verpflichtet, adäquate und effektive Garantien gegen die staatliche Missbrauchsgefahr einzurichten (Uzun gg. Deutschland).

Heute befasst sich der EGMR immer stärker mit den Herausforderungen, die die neuen Technologien des Internets betreffen: also die staatenübergreifenden und intransparenten Wege der Daten im Internet und die daran anknüpfende staatliche Datenbeschaffung, unabhängig davon, ob sich die Daten im In- oder Ausland befinden, des Weiteren auch die internationale Kooperation von Geheimdiensten und extraterritoriale Handlungen der Staaten. Eine der größten Herausforderungen besteht wohl darin, dass sich Meinungsäußerungen und Daten nicht mehr innerhalb des Territoriums und damit in der Jurisdiktion eines Staates bewegen, sondern durch das Internet eine Entgrenzung erfahren haben, die die Zuständigkeit *ratione personae* bzw. *ratione loci* des EGMR und der nationalen Gerichte betreffen. Es gibt noch sehr wenige Internet-Urteile des EGMR, die sich mit grenzüberschreitenden Sachverhalten befassen, nennenswert ist lediglich Perrin gg. Vereinigtes Königreich, in dem das Gericht das britische Recht auch für die elektronische Datenübermittlung im Ausland für anwendbar erklärte. In dem Urteil Bel El Mahi gg. Dänemark hat der EMGR hingegen den erforderlichen „link“ zwischen den Beschwerdeführern in Marokko, welche sich über die Veröffentlichung von Karikaturen Mohammeds in

dänischen Zeitungen beschwerten, und der dänischen Regierung zur Begründung der dänischen Jurisdiktion, nicht gesehen.

In Zeiten der Bedrohung durch terroristische Angriffe und der damit einhergehenden staatlichen Überwachung im Cyberspace und des hohen technologischen Fortschrittes steht der EGMR vor immer neuen Herausforderungen in Bezug auf die Vereinbarkeit solcher Maßnahmen mit dem Recht auf Privatsphäre und der freien Meinungsäußerung und auch dem Verhältnismäßigkeitsgrundsatz. Schließlich ist die Streubreite der Überwachung viel größer und der Kernbereich des Privaten zugänglicher geworden. Auch wird er in Bezug auf die *margin of appreciation* der Mitgliedstaaten im Rahmen der Rechtfertigung solcher Maßnahmen Eckpunkte setzen und die Grenzen dieses Ermessens verdeutlichen müssen.

Die derzeitig beim EGMR anhängigen Fälle im Zusammenhang mit den Enthüllungen der staatlichen Überwachungsmaßnahmen durch Edward Snowden aus dem Jahr 2013 sind besonders anschaulich im Hinblick auf die oben genannten Problemfelder. Darunter sind drei Fälle, die sich mit den *britischen Überwachungsmaßnahmen* und dem sog. Regulation of Investigatory Powers Act ("RIPA") befassen. RIPA ermächtigt die britischen Sicherheitsbehörden zur verdeckten Überwachung von Kommunikation und die Beschaffung, Verwertung und Entschlüsselung von Daten aus dieser Kommunikation. Der Austausch von Ermittlungsergebnisse mit ausländischen Geheimdiensten ist dort nicht geregelt. Die Beschwerdeführer sind allesamt durch diese Enthüllungen darauf aufmerksam geworden, dass sie möglicherweise Gegenstand dieser Überwachungen geworden sind.

Der EGMR muss darüber entscheiden, ob es einer ausdrücklichen gesetzlichen Grundlage in den Mitgliedstaaten bedarf, die die entsprechenden Stellen dazu ermächtigt Informationen mit ausländischen Geheimdiensten zu teilen. Wenn daraus eine Beschränkung der Grundrechte auf Privatsphäre und der freien journalistischen Tätigkeiten folgt, muss dies geboten sein. Zwar gilt der Schutz der nationalen und öffentlichen Sicherheit als Rechtfertigungsgrund für Beschränkungen der Gewährleistungen aus Art. 8 und 10 EMRK, in den derzeit anhängigen Fällen muss das Vereinigte Königreich die Gefahr, die von den Organisationen und Einzelpersonen ausgehen soll, jedoch erst darlegen. Die massenhafte Überwachung, auch von nicht verdächtigen Personen muss den Erfordernissen der Geeignetheit und Erforderlichkeit entsprechen. Die anlassbezogene Überwachung ist jedoch ein milderes und gleich geeignetes Mittel. Und ob die massenhafte Datensammlung dazu führt, dass mehr Straftaten aufgeklärt werden, ist auch heftig umstritten.

Des Weiteren sollte mit Spannung erwartet werden, wie der EGMR in der Sache entscheidet, in der sich Organisationen, die ihren Sitz im Ausland haben und durch den britischen Geheimdienst überwacht wurden, auf die Gewährleistungen aus der EMRK berufen. Das extraterritoriale Handeln der britischen Behörden müsste dazu dem Vereinigten Königreich gem. Art. 1 EMRK zurechenbar sein. Wenn der EGMR mit dem Zurechnungskriterium der „virtual control“ der britischen Behörden arbeitet, dann kann die Verantwortlichkeit des Vereinigten Königreiches für derart extraterritoriale Handlungen bejaht werden. Nach dem Recht der Staatenverantwortlichkeit entspräche dies dem Erfordernis der „effective power and control“, das bei extraterritorialen hoheitlichen Handlungen staatlicher

Einrichtungen durchaus vorliegt. Dieses Zurechnungskriterium kommt auch in der Rechtsprechung des EGMR zur Anwendung (siehe Catan u.a. gg. Moldawien und Russland und Jaloud gg. Niederlande), er beruft sich dabei direkt auf die internationalen Zurechnungsregeln (Hirsi Jamaa u.a. g. Italien). Da es noch an Zurechenbarkeitskriterien im Bereich des digitalen Handelns im Ausland seitens des EGMR fehlt, wird auch diese Entscheidung Klarheit schaffen.

Diese drei Verfahren sind folgendermaßen zusammenzufassen:

In der Sache *Big Brother Watch u.a. gg. das Vereinigtes Königreich* (Beschwerde Nr. 58170/13) wehren sich vier Beschwerdeführer, die sich für den Datenschutz einsetzen, gegen digitale Überwachungsmaßnahmen durch britische Behörden. Sie werfen ihnen vor von dem US-Internet-Überwachungsprogrammen PRISM zu profitieren, indem sie die gesammelten Informationen der NSA erhalten und auch eigene Überwachungsprogramme eingesetzt haben. Dadurch würden sie in ihrem Recht aus Art. 8 EMRK verletzt. Die Beschwerdeführer bringen vor, dass es keine Rechtsgrundlage dafür gebe, dass britische Behörden Geheimdienstinformationen in Bezug auf elektronische Kommunikation von ausländischen Geheimdiensten erhalten dürfen. Es gebe auch keine nationalen Mechanismen zur Kontrolle und Absicherung dieses Informationsaustauschs, durch den die britischen Behörden die Daten erhalten, weiterverarbeiten und speichern.

Der EGMR fordert in solchen Fällen, dass das Gesetz zur heimlichen Überwachung hinreichend bestimmt und klar ist und dabei die Rechtsfolgen vorhersehbar sind. Des Weiteren

muss das Gesetz das Ermessen der Behörden und dessen Reichweite hinreichend klar formulieren, um den Bürger vor Willkür zu schützen (Weber und Saravia gg. Deutschland). Die Beschwerdeführer rügen, dass der Rechtfertigungsgrund der nationalen Sicherheit zu vage und undeutlich und die staatlichen Sicherungsmechanismen nicht angemessen seien. Des Weiteren sei die flächendeckende Übertragung dieser Kommunikationsdaten von unzähligen Personen über das transatlantische Glasfaserkabel ein unverhältnismäßiger Eingriff in das Recht auf Privatsphäre von Millionen Menschen. Der EGMR hat in der Sache *Klass* betont, dass die heimliche Überwachung im Sinne der nationalen Sicherheit nicht so weit gehen darf, dass sie im Ergebnis die Demokratie aushebelt oder gar zerstört. Vor diesem Hintergrund und angesichts der Streubreite der Überwachung ist zu erwarten, dass der EGMR dies im Zuge dieser Beschwerde berücksichtigen wird.

In dem Fall *Bureau of Investigative Journalism and Alice Ross* (Beschwerde Nr. 62322/14) liefern die Beschwerdeführer (eine gemeinnützige Organisation und eine Angestellte) hochwertigen Journalismus im öffentlichen Interesse. Sie berichten über sensible Themen wie nationale Sicherheit, Korruption, staatliche Überwachung, den Krieg gegen den Terrorismus und die Machenschaften des britischen Geheimdienstes. Durch die Sammlung der Kommunikations- und Metadaten durch die Überwachungsprogramme fühlen sie sich in ihrer Meinungsfreiheit und Arbeit als Journalisten und in ihrem Recht auf Privatsphäre beeinträchtigt. Es fehle an einer gesetzlichen Grundlage für das Vorgehen und sie sehen ihre Rolle als investigative Journalisten und die sog. *watchdog*-Funktion der Presse in Gefahr. Die flächendeckende Überwachung, die Speicherung und Verwendung der Daten seien daher unverhältnismäßig.

Eine weitere Beschwerde gegen das Vereinigte Königreich (Beschwerde Nr. 24960/15) wurde von 10 Menschenrechtsorganisationen eingereicht, die mit Politikern, Journalisten, Anwälten, Opfern von Menschenrechtsverletzungen und Whistleblowern auf digitalem Wege kommunizieren. Der Inhalt dieser Kommunikation ist meist sehr sensibel und vertraulich. Sie haben ihre Sitze teilweise in England, in Europa und außerhalb von Europa. Sie befürchten, dass sie durch die britischen Behörden mit dem Programm TEMPORA oder durch die NSA mit dem Programm PRISM überwacht werden und sehen sich durch die britische Überwachungstätigkeit in ihren Rechten aus Art. 8 und 10 EMRK verletzt.

In allen Fällen hält die britische Regierung die Überwachung für gerechtfertigt, da sie im Einklang mit dem Recht erfolgt und im Sinne der nationalen Sicherheit erforderlich seien. Im Hinblick auf den Erhalt der Informationen der NSA beruft sich die Regierung darauf, dass es für den Austausch von Informationen durch Geheimdienste keiner ausdrücklichen gesetzlichen Grundlage bedürfe. Es reiche aus, dass entsprechende interne Regeln oder Vorgaben existieren und öffentlich bekannt seien.

*Layla Kristina Jaber ist wissenschaftliche Assistentin am Lehrstuhl für Öffentliches Recht und Rechtsphilosophie der Universität Mannheim und Doktorandin an der Universität Heidelberg. Das Thema der Doktorarbeit liegt im Bereich der Individualsanktionen des Sicherheitsrates der Vereinten Nationen und der Verfahrensrechte der EMRK.*

*Dieser Beitrag wurde im Rahmen des Kolloquiums "Digitale Überwachung und Cyberspionage: deutsch-französische Perspektiven", welches vom 22. bis 23. September in Paris*

stattfind, präsentiert. Weitere Beiträge aus dem Kolloquium finden sich nebst dem Völkerrechtsblog ([hier](#)) auch [hier](#) und [hier](#).

ISSN 2510-2567

**Tags:** Cyber, Digitalization, European Court of Human Rights, Human Rights



Print



Facebook 14



Twitter



Email

#### Related

Die schwierige Aufgabe der Humanisierung des humanitären Völkerrechts:  
17 June, 2015  
In "Discussion"

Keine Diktatur der Volksherrschaft!  
12 December, 2014  
In "Symposium"

Verstoß von Deutschland gegen EMRK wegen mangelnder Untersuchung von Polizeigewalt  
1 December, 2017  
In "Current Developments"

PREVIOUS POST



The surveillance you have paid for

NEXT POST

Unilateralism ahead?





## No Comment

Leave a reply

Logged in as ajv2016. Log out?

**SUBMIT COMMENT**

---

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.